ICS 11.040.50
CCS C 43

YY

中华人民共和国医药行业标准

YY/T XXXX-XXXX

CT影像处理软件通用技术条件

General specification of CT image processing software

（草案稿）

20XX-XX-XX 发布　　20XX-XX-XX 实施

国家药品监督管理局　发布

前　言

本文件按照 GB/T 1.1—2020 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由国家药品监督管理局提出。

本文件由全国医用电器标准化技术委员会医用 X 射线设备及用具分技术委员会（SAC/TC10/SC1）归口。

本文件起草单位：

本文件主要起草人：

CT影像处理软件通用技术条件

1 范围

本文件规定了CT影像处理软件产品的术语和定义、要求和试验方法。

本文件适用于CT影像处理软件及包含CT影像后处理功能的医疗器械软件。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 9706.1-2020 医用电气设备 第1部分：基本安全和基本性能的通用要求

GB 9706.244—2020 医用电气设备 第2-44部分：X射线计算机体层摄影设备的基本安全和基本性能专用要求

GB/T 25000.10—2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE）第10部分：系统与软件质量模型

GB/T 25000.51—2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE）第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则

YY/T 1708.1—2020 医用诊断X射线影像设备连通性符合性基本要求 第1部分：通用要求

YY/T 1766.3—2023 X射线计算机体层摄影设备 图像质量评价方法 第3部分：双能量成像与能谱应用性能评价

YY/T 1833.1—XXXX 人工智能医疗器械质量要求和评价 第1部分：术语

ISO/IEC/IEEE 24765—2017 Systems and software engineering—Vocabulary

3 术语和定义

GB 9706.244—2020、YY/T 0664—2020、GB/T 25000.10—2016和GB/T 25000.51—2016、YY/T 1766.3—2023界定的以及下列术语和定义适用于本文件

3.1

CT影像处理软件 CT image processing software

对CT影像进行可视化、分割、测量、分析等后处理的医疗器械软件。

注：CT影像不包含CT扫描过程中形成的投影图像等中间环节的影像。

3.2

随附文件 accompanying document

随软件所带的文件，其内容包含了为责任方或操作者提供的信息。

3.3

元数据 metadata

包含在影像文件中的影像像素以外的辅助信息，可能包括患者信息、设备信息、影像参数信息等。

3.4

操作者 operator

操作软件的人

注：操作者可以是软件临床功能的使用者，也可以是以配置、管理、维护为目的与软件进行交互的人。

[来源：GB/T 9706.1—2020，有修改]

3.5

责任方 responsible organization

对某软件的使用和维护负有责任的实体。

[来源：GB/T 9706.1—2020，有修改]

3.6

影像视窗 image view port

用于显示影像的最小界面单元。

3.7

事务 transaction

在测试中划分的若干请求的集合，通常代表一个功能点或工作流。

3.8

最大并发事务数 maximum concurrent transaction

事务吞吐量达到最大值时，软件所承受的并发事务数。

3.9

事务吞吐量 transaction throughput capacity

在单位时间内软件能够处理完成的事务量，单位是TPS（每秒事务数，S也可替换为M（分钟）、H（小时）等）。

3.10

影像处理容量 image processing capacity

对于指定的影像处理或影像存储功能，软件能够处理的单次最大数据量。

3.11

事务响应时间 transaction response time

操作者发起一个事务开始，服务器完成对该事务的请求的处理并返回处理结果所经过的时间。

3.12

事务成功率 transaction success rate

正确执行的事务数与全体事务数的比率。

3.13

客户端/服务器架构 client/server architecture

C/S架构 C/S architecture

使用专用的应用程序作为客户端，分布式的客户端和集中式的服务器之间通过网络进行通信实现的计算架构模型。

3.14

浏览器/服务器架构 browser/server architecture

B/S架构 B/S architecture

使用通用的浏览器作为客户端，分布式的客户端和集中式的服务器之间通过网络进行通信实现的计算架构模型。

注：B/S架构是由C/S架构发展而来的特例模型，在本文件中所称的C/S架构不包含B/S架构。

3.15

单机架构 single-tier architecture

所有数据处理均在同一台计算机中实现的计算架构模型。

3.16

P2P 架构 peer-to-peer architecture

不存在集中式的服务器，由不同节点相互之间直接进行网络通信、数据处理和资源共享的去中心化的计算架构模型。

3.17

终端 terminal

C/S 架构与 B/S 架构中的客户端、单机架构中的计算机与 P2P 架构中的节点的统称。

3.18

用户界面 user interface

UI

软件与操作者之间进行信息交换的界面

3.19

交互元素 interactive element

支持操作者主动发起人机交互的 UI 元素

3.20

工具提示 tooltip

当用户将鼠标悬停在某个元素上时，以文本形式显示该元素的相关信息。

3.21

标注标识 annotative dimension

叠加在影像上用于标示与位置有关的发现、测量结果、测量基准的图形、文字或符号

3.22

工作流 workflow

为了执行一个具体的任务，在软件中设计的一系列 UI 交互与计算过程的集合。

3.23

物空间 object space

患者被扫描部位所处的物理空间。

注1：在本文件中，物空间在扫描发生的瞬间被同时以“快照”的形式确立，并不考虑扫描后物空间的变化。

注2：物空间的坐标系建立参见GB 9706.244—2020中的图201.101

3.24

像空间 image space

原始 CT 影像及经过可视化后处理的影像视窗中，由离散像素和相关的元数据建立的影像空间。

注：原始CT影像中的影像空间坐标系通常由影像元数据定义。

3.25

原始像空间 original image space

原始 CT 影像的像空间。

4 要求

4.1 通则

4.1.1 软件功能边界

对于软件所定义的每种角色的操作者而言，软件功能的边界应是清晰明确的，边界可在随附文件中进行指明或通过访问控制机制限制。

4.1.2 规定运行依赖于必备软硬件的处理软件

当软件的运行依赖于其他必备软硬件时，对于本文件的符合性可通过与相应的必备软硬件共同实现，此时相应必备软硬件的随附文件应被视为处理软件随附文件的一部分。随附文件应声明此情形。

4.1.3 测试数据兼容性

随附文件中应规定软件或某项软件功能所支持处理的影像数据要求，例如影像文件元数据满足特定约束条件的影像、使用指定扫描协议生成的影像、通过指定的必备软硬件输出的影像等。

4.1.4 数据鉴别

规定了影像文件元数据要求的处理软件应具备相应元数据识别的能力，并按照随附文件中的约束条件进行判断。

当测试数据不符合元数据约束条件时，软件应拒绝进行处理，并给出包含相应元数据信息的提示。

对于推荐但不是必要的元数据约束条件，软件可给出提示，并由操作者选择是否继续执行处理工作流。

4.1.5 数据清洗

对于指定扫描协议、指定必备软硬件及其他影像数据本身不直接包含数据兼容性判定依据的情形，测试者应当使用适当的方法确保使用的测试数据满足随附文件中的影像数据要求。

注：这种影像数据兼容性的判定可通过信息完善且可追溯的影像数据库实现。

4.1.6 测试集

对于每项软件功能，测试集中至少应当包含 3 套符合测试数据兼容性要求的影像数据，但同一套影像数据可以出现在满足要求的多项软件功能的测试集中。

如包含相应要求，测试集中的测试数据应覆盖以下元数据的最大值和最小值：

——平面内像素间距

——平面内重建矩阵

——层间距

——层数

——存储位深

注：当元数据的允许范围不包含边界值时，应当选择尽可能接近的值

4.1.7 测试边界

当软件预期处理 CT 影像以外的其他模态影像（如 MR、PET、DR 等）时，依据本文件进行的测试不包括专门用于其他模态影像的处理功能，但包括能够同时用于 CT 影像和其他模态影像的处理功能。

4.2 随附文件

4.2.1 通则

随附文件的不同文档，或一份文档中的不同部分，可预期供特定角色的操作者进行阅读，

4.2.2 软件使用的指导

随附文件应对软件中所有预期由操作者使用的功能提供操作指导。

当某一用户交互组件（如：按钮、对话框等）在 UI 中具有名称或标题时，随附文件对应使用该名称或标题对组件进行指称。

4.2.3 风险警示

对于以下情形，随附文件中应给出风险警示：

——影像处理功能输入的局限性，尤其是未通过数据鉴别机制进行判断的输入数据约束条件；

——影像处理功能输出用于临床决策的局限性。

4.3 功能性

4.3.1 功能完备性

包含特定预期用途的软件至少应包含表 1 所列出的功能。

表 1 CT 影像处理软件的功能要求

特定预期用途	应包含的功能
制定骨科手术计划	区域分割、MPR、MIP、三维重建
制定软组织手术计划	区域分割、MPR、三维重建（具体绘制）
头部影像可视化	区域分割、MPR、CPR、三维重建（具体绘制）
肺部及呼吸道影像可视化	区域分割、MIP
心脏影像可视化	区域分割、MPR、CPR、三维重建
腹部器官可视化	区域分割、三维重建（具体绘制）
血管（增强及灌注）可视化	区域分割、MPR、CPR
多模态影像处理	图像配准、图像融合

4.3.2 功能正确性

4.3.2.1 窗宽窗位

窗宽窗位变换后图像灰度值应能覆盖显示器支持的最大/最小灰度范围。

窗宽窗位变换应当为线性变换。

无论使用何种方式进行调节，窗宽/窗位指示器中的数字应当实时同步。

4.3.2.2 区域分割

4.3.2.2.1 通则

区域分割应使用交并比、Dice 系数或豪斯多夫距离进行算法性能评价。

使用覆盖软件支持的全部待分割区域的测试影像进行测试。

4.3.2.2.2 基于阈值的分割方法

软件应有措施保障分割区域的连通性与完整性。

软件应包含对阈值相似的非待分割区域进行排除的方法，如果这一方法是操作者手动执行的，应在随附文件或 UI 中告知操作者。

通过包含较大噪声的影像、待分割区域存在高对比度间隙的影像、待分割区域与影像中其他区域 CT 值存在交集的影像进行测试。

4.3.2.2.3 基于区域生长的分割方法

如果种子点是由操作者进行选取的

4.3.2.2.4 基于图论的分割方法

如果软件采用了先验形状作为分割基准，当待分割区域无法匹配先验形状时软件应拒绝处理或在随附文件中给出与先验形状的必要特征有关的说明。

4.3.2.2.5 基于深度学习的分割方法

当待分割区域部分缺失、畸形或 CT 值与常规水平具有较大差异时，软件应能正确实施分割或在随附文件中明确排除相应情形的影像兼容性。

4.3.2.2.6 分割区域的手动创建与修改

区域分割功能预期用于进行三维重建、制定手术计划或制定放疗计划，软件还应支持分割区域的手动修改。

手动修改方式应使得分割区域包含或排除任何像素均不受到限制。

注：例如支持精确到像素的增量和减量的自由绘制即满足上述要求，而基于半自动边缘吸附的轮廓控制点拖动则不满足上述要求。

4.3.2.2.7 区域识别

当软件支持分割区域自动识别为人体器官或组织的功能时，应支持手动对识别标记结果进行修改，如果修改值是从列表中选取的，其范围至少应覆盖支持自动识别的所有部位。

当一系列区域具备序列关系时（如肋骨或椎骨），其识别标记不应强制连续。

注：例如患者肋骨缺失的情形。

如果区域识别标记叠加在影像上，应支持标记位置的移动和标记与分割区域关联关系的指示。

4.3.2.3 图像配准与融合

对于每一项配准功能，软件界面或随附文件应指明：

——其为刚性配准或非刚性配准；

——配准所支持的影像或非影像元素类型（例如：影像模态、预置的几何模型）；

自动的刚性配准应支持手动的旋转、平移、缩放修改。

4.3.2.4 三维重建

4.3.2.4.1 通则

如果三维重建的影像预期用于制定手术计划，三维重建的分辨率不应低于原始 CT 影像。

注：当原始CT影像xy方向与z方向的像素大小不一致时，三维重建的重采样分辨率应当以最小者为基准。

4.3.2.4.2 面绘制

如果面绘制算法对所选择的分割区域进行了修补，用户界面或随附文件应指出三维重建影像与原始分割区域的非对应性。

4.3.2.4.3 体绘制

除非体绘制功能仅用于单一的具体用途（例如：通过内置的渲染模板生成特定部位的体绘制影像）应支持对不同的分割区域分别设置颜色遮罩编码与透明度。

4.3.2.5 能谱应用

4.3.2.5.1 通则

对于每项能谱应用功能，随附文件应指明其支持的双能量成像模式。

4.3.2.5.2 能谱应用的性能评价

应符合 YY/T 1766.3—2023 中 8.5 的要求

测试所使用的影像应覆盖每种支持的双能量成像模式。

4.3.2.6 几何测量功能

4.3.2.6.1 通则

处理软件中的几何测量功能应符合以下要求：

——当在影像视窗中叠加显示几何测量值时，测量的标注标识应与测量值保持同时可见；

——在一个影像视窗中存在多个测量时，操作者应能获取每个测量的标注标识与测量值的对应关系；

——已绘制的测量数值不应受影像缩放、平移、旋转等操作的影响；

——影像上的测量标注标识不应随着对影像的平移、翻转、缩放等操作而改变与影像间的相对位置和尺寸关系；

——对于建立在几何测量基础上的软件测量结果（如：射血分数、狭窄率等），随附文件应给出测量结果的计算方法。

4.3.2.6.2 在非刚性变换的影像中进行几何测量

在非刚性变换的影像（如 CPR、骨骼展开）中，每个像素对应的物空间中的各向尺度均可能是不同的，且测量几何形状的标注标识在像空间与物空间的形状也存在差异（例如：像空间中的直线测量在物空间中是一条曲线），软件应：

——禁止在非刚性变换中进行几何测量，或

——确保测量的准确性以及操作者对测量理解的正确性：

- 使用数字模体对测量准确性进行验证，结果应符合制造商的要求；
- 使用测量工具的名称和工具提示确保操作者正确理解测量的意义；

示例：工具名称：沿曲面长度测量，工具提示：在沿曲面展开的图像中测量血管的走行长度。

- 在影像视窗中显示非刚性变换的影像信息。
- 如果其他不同的影像视窗中也显示了此几何测量的标注标识，应确保

示例：在体绘制三维重建影像视窗中显示沿血管走行的测量标注标识。

4.3.2.6.3 在三维重建的影像中进行几何测量

随附文件应给出几何测量控制点的锚定方法。

示例：在面绘制三维重建影像中，几何测量控制点的锚定点为当前显示面上距离鼠标点击位置最近的三角面顶点。

4.3.2.6.4 测量不确定度

使用CT影像处理软件执行的测量功能，大部分来自于采集影像所使用的CT设备与患者（例如：心脏的跳动），但对于操作者与处理软件交互和处理软件自身贡献的测量不确定度，随附文件中应给出评价所需的必要信息：

a) 像素锚定导致的不确定度分量，这一分量来自用户通过鼠标点击或其他方式确定几何测量的锚点时，用户视觉空间坐标系中的位置与经过系统采集和转换后在像空间坐标系（或为测量功能单独建立的测量几何空间）中锚点的位置的差异。该不确定度受到影像视窗占用的显示器像素矩阵、影像像素对应的空间尺度、影像的缩放状态、锚点占用的显示器像素矩阵影响。

b) 数值修约导致的不确定度分量，这一分量来自确定锚点后，对几何测量结果的计算过程中所使用的变量精度，以及测量值显示的数值精度。

c) 灵敏度系数的计算，需要建立原始CT影像中的参数与几何测量结果之间的数学模型，用于计算不确定度分量的灵敏度系数。

注：4.3.2.6.1第五破折号的要求可以支持建立几何测量结果与其他软件测量结果之间的数学模型。

4.4 易用性

4.4.1 操作者所需信息的指示

当前软件运行存在关键性错误，导致以下问题时，软件UI应给出错误的具体情形，以及如何解决该错误的建议，或给出能索引至随附文件中的相应信息的唯一标识：

——无法执行连贯工作流的下一步骤；

——非用户主动放弃的数据将会丢失，且无法恢复；

——软件无法给出预期的处理结果；

当所需显示的信息超出UI为此信息设定的显示区域范围时，应有方法获得完整的显示信息。

注：例如通过鼠标悬停后的浮出窗口，或通过可变的显示区域大小等。

如果某一影像视窗所显示的影像存在额外的叠加遮罩或不同于原始影像的非线性像素值重映射，应当在影像视窗区域内指明当前显示的状态信息。

注：窗宽/窗位的调节通常是线性的，而非线性的像素值重映射往往用于非常具体的一项可视化用途。

4.4.2 工作流约束

对于工作流中具有明确顺序要求的步骤，软件应限制操作者使用错误的顺序。

4.5 性能效率

4.5.1 容量

4.5.1.1 最大并发事务数

随附文件中应给出软件在指定的运行环境下最大并发事务数，当软件以组件形式运行于底层平台上时，可索引至底层平台随附文件的相应内容。

最大并发事务数应与测试工作流、事务吞吐量、事务响应时间与允许的最低事务成功率一并给出，其中事务成功率不应低于 90%。

软件的最大并发事务数、事务吞吐量、事务响应时间、事务成功率及其资源利用性（参见 4.5.3）应符合随附文件中的要求。

通过检查随附文件，软件测试，必要时检查软件的设计开发、验证与确认文档，及以下方法来检验是否符合要求。

测试工作流应包括：

a) 影像加载；

b) 执行自动后处理功能；

c) 提交后处理结果。

如果某一工作流包含无操作者交互的算法预处理阶段（例如：对所有符合条件的影像自动执行分割算法），则该预处理功能单独作为事务进行并发测试。

当存在缓存时，最大并发事务数测试应关闭缓存功能或对查询的信息和读取的影像进行参数化以确保每个虚拟用户每次请求的信息都是不同的。

在测试过程中，应对事务吞吐量、事务响应时间以及事务的成功率进行监控。

在测试中可不设置集合点。

测试的持续时间应保证成功执行的事务总数大于最大并发事务数的 4 倍，并不低于 5 分钟。

应使用等于随附文件中规定的最大并发事务数 100%的虚拟用户及 90%的虚拟用户分别进行并发测试，如前者的事务吞吐量小于等于后者，视为并发测试失败。

应在关键步骤中设计适当的断言以判断结果的正确性，从而计算事务成功率，而非仅通过请求返回的类型（例如：http 请求响应为 200）进行判断。

4.5.2 时间特性

随附文件中应给出软件在指定的运行环境下的事务响应时间，

软件的时间特性及其资源利用性应符合随附文件中的要求。

通过检查随附文件，软件测试，必要时检查软件的设计开发、验证与确认文档，及以下方法来检验是否符合要求。

被测事务应涵盖软件的典型工作流。

软件的时间特性应在随附文件中的规定的典型处理条件下进行，如未规定，应在最大影像处理容量及最大并发数下进行。

当进行并发的时间特性测试时，应在每一个被测事务开始时设定集合点。

在测试时间特性时，应关闭“预加载”等功能并清除缓存，如果预加载功能是不可关闭的且无法与影像导入或读取的过程进行区分，则将影像导入或读取时间纳入时间特性统计范围内。

如果开始与终止是基于操作者交互的，应以操作者交互输入的时间点作为开始时间，以向操作者完成预期输出的时间点作为终止时间。如中间过程存在操作者交互，应在结果中去除人为操作的时间。

4.5.3 资源利用性

随附文件应给出软件在指定的运行环境下的资源利用性约束，至少包括：平均 CPU 占用率。

通过检查随附文件，软件测试，必要时检查软件的设计开发、验证与确认文档，及以下方法来检验是否符合要求。

软件的资源利用性测试执行的工作流可与 4.5.1.1 与 4.5.2 的测试相同，并在相应的测试中同时进行。

对于 C/S 或 B/S 架构的软件，资源利用性测试监控的对象仅包括被测软件服务器端。

4.6 网络安全

4.6.1 自动注销

基于 C/S 或 B/S 架构的处理软件，客户端的身份鉴别信息应有时间限制。

具有可交互的图形化界面的处理软件应具备基于闲置时间的自动注销功能。

自动注销状态下，健康数据应不可见。

自动注销后，用户再次登录时，未保存的数据与未完成的工作流不应丢失。

自动注销后操作者应需要再次进行用户身份鉴别才能登录软件。

4.6.2 审计

软件应具有记录健康数据的调阅、修改和删除事件有关的审计信息的能力。

软件应在面向具有审计日志查阅权限的用户的文档中给出日志关键字信息，应包括所有日志关键字的含义、生成条件和生成格式。

审计日志应不可修改，所记录的信息应确保可以追溯到具体的用户、时间和事件。

如审计日志能够被软件发送给其他媒介或终端，应有方法确保传输过程的保密性和完整性。

通过软件测试，必要时检查软件的网络安全相关文档，及以下方法来检验是否符合要求。

测试用例的设计应遍历每一个日志关键字，以及在进行全部功能性、网络安全测试后查看文档中的日志关键字信息是否包含了所有网络安全日志。

通过尝试对网络安全日志进行编辑、修改系统日期从而实现盖写等操作进行测试。

4.6.3 授权

软件应能对存储的影像进行访问授权，以控制用户仅能访问其有权限访问的影像。

软件在数据访问授权时，应考虑最小数据授权原则，仅提供完成预期用途所必需的健康数据的授权，或向用户提供实现该原则的必要设置选项。

预期用于访问指定患者影像的授权凭据不应仅使用与患者身份绑定的信息。

注：例如：使用完整的身份证号即可查阅对应患者的影像信息。

授权凭据不应硬编码于软件中。

每次从新设备访问需要进行授权的数据时，应要求用户重新提交授权凭据，即便这些数据是经由已被授权的用户转发的。

通过软件测试及必要时检查软件的网络安全相关文档来检验是否符合要求。

4.6.4 节点鉴别

使用 DICOM 协议进行通信时，软件应能设置合法访问节点的应用实体名称（AE Title），宜能设置合法访问节点的 IP 地址、端口号等信息。

软件应支持对应用实体权限的控制。

注：如 C-FIND、C-MOVE、C-Store、Filming、MPPS、Worklist 等权限配置。

通过软件测试及必要时检查软件的网络安全相关文档来检验是否符合要求

4.6.5 人员鉴别

软件应支持对每一个用户提供各自的鉴权凭证。

对于使用额外的硬件进行人员鉴别时（如指纹传感器、读卡器、虹膜传感器等），随附文件中应指定对鉴别设备的要求、与软件的连接方式以及如何加密。

通过软件测试及必要时检查软件的网络安全相关文档来检验是否符合要求。

4.6.6 连通能力

随附文件中应指明使用本软件所必需的硬件连通能力。

随附文件中应给出软件占用的网络端口以及软件与其他软件、软件各组件之间的传输协议。

对于支持 DICOM 传输协议的软件，见 4.7.1。

通过检查随附文件，软件测试，必要时检查软件的网络安全相关文档，及以下方法来检验是否符合要求。

对于硬件连通能力的要求，仅应考虑必须具备的连接。

示例：当软件必须通过 USB 接口控制指定的医疗器械硬件时，USB 接口视为必需的硬件连通能力；当软件能够通过操作系统的文件 I/O 功能向 U 盘存储文件时，USB 接口不视为必需的硬件连通能力。

4.6.7 物理防护

以云服务形式交付的软件，随附文件中应指明部署环境的物理防护形式。

通过检查随附文件及必要时检查软件的网络安全相关文档来检验是否符合要求。

4.6.8 系统加固

随附文件应就如何关闭或禁用软件运行所不需要的端口、通讯协议、服务、应用程序或引导程序给出必要的说明。

以云服务形式交付的软件，随附文件应指明部署环境的等级保护级别。

通过检查随附文件及必要时检查软件的网络安全相关文档来检验是否符合要求。

4.6.9 数据去标识化

将影像传输到软件之外（包括文件形式的传输行为和数据流形式的影像呈现行为）时，软件应具有去标识化的功能，去标识化字段应至少包括患者姓名、患者唯一标识、患者地理位置信息、患者联系方式、医疗机构名称、医疗机构地址。

去标识化功能宜进行分级，允许操作者选择需要的字段或预置的字段组合进行去标识化。

当影像的接收方是影像后处理应用程序，且其后处理结果预期仅回传给本软件时，应支持传输去标识化以及接收恢复标识化功能。

注：该功能可允许影像传输经过不受信任的网络、节点或终端时，将去标识化程度提升至最高。

通过软件测试及必要时检查软件的网络安全相关文档来检验是否符合要求。

4.6.10 数据完整性与真实性

制造商应给出软件保障数据完整性的措施。

以非授权方式更改用户访问控制设置（包括用户名/密码表、密码尝试次数设置、用户权限设置等）、影像传输设置（包括节点白名单、传输协议设置、加密设置等）、影像存储设置（包括允许的存储形式、存储匿名机制等）的行为应：

——被阻止，或

——被识别并以适当的形式通知用户。

支持多家医疗机构共用云服务的软件，应能确保各个机构的数据隔离性、可靠性和完整性，并应能不受不同医疗机构的患者 ID、检查号重复的影响。

通过软件测试，必要时检查软件的网络安全相关文档，及以下方法来检验是否符合要求。

根据制造商给出的数据完整性保障措施设计测试用例进行测试。

4.6.11 数据备份与灾难恢复

当数据备份与恢复功能预期用于防范计算机系统遭到非预期的破坏时，随附文件应对备份数据的安全保存给出必要的信息。

备份与恢复功能的要求见 4.4.1。

通过检查软件的网络安全相关文档来检验是否符合要求。

4.6.12 数据存储保密性与完整性

患者健康数据以及未去标识化的影像数据存储于公有云环境时，其内容应被加密。

软件应能识别出对用户授权数据、审计日志数据以及其他与网络安全能力有关的数据的完整性产生损害的事件，且能够提供记录这些事件并使授权用户获知的方法。

通过软件测试及必要时检查软件的网络安全相关文档来检验是否符合要求。

4.6.13 数据传输保密性

患者健康数据以及未去标识化的影像数据通过公网传输时，传输过程应有加密措施。

患者健康数据以及未去标识化的影像数据通过局域网传输时，传输过程可具有加密措施。

通过软件测试及必要时检查软件的网络安全相关文档来检验是否符合要求。

4.6.14 数据传输完整性

由操作者发起的，同时发送或接收多幅影像的行为应有影像序列完整性检查机制，并就完整性检查结果给出相应提示。

将数据通过公网进行传输的软件，应有确保影像及患者健康数据传输过程完整性的措施。

支持分布式存储或数据同步功能的软件，应能确保影像数据的一致性；检索和调阅时，对尚未同步的数据，应提供适当的状态指示。

通过软件测试及必要时检查软件的网络安全相关文档来检验是否符合要求。

4.6.15 网络安全补丁升级

当软件预期不接入互联网时，随附文件应告知用户检查与执行运行环境及软件自身的安全缺陷修复程序的必要性。

通过检查随附文件及必要时检查软件的网络安全相关文档来检验是否符合要求。

4.6.16 软件物料清单

软件应能显示已安装的所有组件及其版本信息。

当已安装的组件发生变化时，显示的组件及版本信息应相应更新。

通过软件测试及必要时检查软件的网络安全相关文档来检验是否符合要求。

4.6.17 现成软件维护

随附文件应对软件所包含的现成软件及如何获取这些现成软件的网络安全更新给出必要的说明。

通过检查随附文件及必要时检查软件的网络安全相关文档来检验是否符合要求。

4.6.18 网络安全指导

宜向承担不同级别的网络安全职责的操作者分别提供各自的随附文件。

注：医疗 IT 系统的管理员与医生承担着不同级别的网络安全职责。

随附文件应给出当用户发现产品的网络安全漏洞时，向制造商反馈的途径。

通过检查随附文件及必要时检查软件的网络安全相关文档来检验是否符合要求。

4.6.19 网络安全特征配置

当任何一项网络安全要求的满足受到用户设置的影响时，随附文件应解释这些设置的方法与结果。

注：这些设置可能包括用户权限设置、去标识化设置和加密设置等。

通过检查随附文件及必要时检查软件的网络安全相关文档来检验是否符合要求。

4.6.20 紧急访问

软件可具有紧急访问功能，在无用户授权的情况下访问软件的指定功能。

紧急访问可具有专用凭据，该凭据不被认为是用户访问控制机制的一部分。

如软件具有紧急访问功能：

根据预期使用场景，紧急访问应通过适当的方式实现最小数据授权原则，以确保通过紧急访问功能登录的用户仅能访问预期使用场景中必要的影像。

示例 1：紧急访问时仅能访问新增数据，无法访问历史数据。

示例 2：紧急访问时需要通过一个或多个精确条件进行检索方能访问符合条件的数据，不支持空的检索条件以及模糊的检索条件。

紧急访问行为、使用的凭据以及所访问的影像数据应有审计日志记录。

可支持禁用紧急访问功能。

通过软件测试及必要时检查软件的网络安全相关文档来检验是否符合要求。

4.6.21 远程访问与控制

应使用不低于 32bit 真彩色或 8bit 灰阶的方式提供预期用于诊断的远程影像显示，

当远程影像显示不满足色彩、灰阶、分辨率的最低要求时，应给出提示。

当使用灰阶方式提供远程影像显示时，随附文件中应给出有诊断价值的信息可能会丢失的说明。

通过软件测试及必要时检查软件的网络安全相关文档来检验是否符合要求。

4.6.22 恶意软件探测与防护

以云服务形式交付的软件，随附文件中应指明部署环境所使用的恶意软件探测与防护软件及其引擎与特征库版本的查看方法。

除非以非 DICOM 格式存储影像数据或将影像数据直接以二进制形式存储在数据库中，软件应有 DICOM 导言内容鉴别机制：

——直接将所有导言内容置为 00H；

——或以白名单的形式将允许的导言内容保留，将白名单以外的导言置为 00H；

——或能鉴别可执行类型的导言内容，将其置为 00H。

这个鉴别机制可以发生在接收/导入影像数据时或发送/导出影像数据时。

通过检查随附文件、软件测试及必要时检查软件的网络安全相关文档来检验是否符合要求。

参 考 文 献

[1] GB 9706.1—2020 医用电气设备 第1部分：基本安全和基本性能的通用要求
[2] YY/T 1833.1—2022 人工智能医疗器械质量要求和评价 第1部分：术语
[3] ISO/IEC/IEEE 24765:2017 Systems and software engineering—Vocabulary